Resultants of Skewly Composed Polynomials

Manfred Minimair*
Seton Hall University
Dept. of Mathematics and Computer Science
South Orange, New Jersey 07079, USA
manfred@minimair.org

ABSTRACT

This paper studies resultants of skewly composed polynomials, obtained from n homogeneous polynomials by replacing their variables with $n+1$ other homogeneous polynomials, called the inner components. It is shown that the resultant of such composed polynomials is a nested resultant where the inner resultant only depends on the inner components. This work can be considered as a continuation of Jouanolou's and Cheng/McKay/Wang's works on resultants of composed polynomials, who consider non-skewly composed polynomials obtained by composing n homogeneous polynomials with n homogeneous polynomials. Interestingly, in their case the composition structure causes the resultant of composed polynomials to be a power product of resultants, whereas in the current work it is a completely different nested resultant.

Categories and Subject Descriptors

I.1.1 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Expressions and Their Representation*

General Terms

Theory

Keywords

Composition, Composed Polynomial, Skewly Composed, Resultant

1. INTRODUCTION

Resultants have been extensively studied [12, 23, 6, 4, 7, 15, 17, 24, 8, 18, 33, 22, 11, 2, 20] because they are fundamental in solving systems of polynomial equations. Recent research is focused on utilizing structure of polynomials, naturally occurring in real life problems, for example, Newton polytope structure and sparsity [34, 14, 13, 10, 5, 35, 3, 30, 20] as well as composition [25, 17, 26, 8, 19, 16, 28, 27, 29, 9]. This paper is part of the author's work studying how resultants are affected by composition structures. The problem considered in the current paper is entirely different from the ones of the previous papers [16, 28, 27, 29, 31, 32, 9] by the author and his co-author's.

Let us start with some introductory remarks concerning the problem. Jouanolou [17] and Cheng/McKay/Wang [8] studied the projective (dense, Macaulay) resultant of composed polynomials $h_1 = f_1 \circ (g_1, \ldots, g_n), \ldots, h_n = f_n \circ (g_1, \ldots, g_n)$. Note that the composed polynomial h_i is obtained from the homogeneous polynomial f_i in the variables $y_1, \ldots, y_n$ by replacing, for all j, the variable y_j with the homogeneous n-variate polynomial g_j. It is shown in [17, 8] that

$$\begin{aligned}\mathrm{Res}_{d_1 e, \ldots, d_n e}(h_1, \ldots, h_n) = \\ (\mathrm{Res}_{d_1,\ldots,d_n}(f_1, \ldots, f_n))^{e^{n-1}} \times \\ (\mathrm{Res}_{e,\ldots,e}(g_1, \ldots, g_n))^{d_1 \cdots d_n},\end{aligned}$$

where d_i is the total degree of f_i, e is the total degree of the g_j's and, as usual, $\mathrm{Res}_{d_1,\ldots,d_n}(f_1, \ldots, f_n)$ denotes the projective resultant of the polynomials $f_1, \ldots, f_n$.

The current paper carries on the works of Jouanolou and of Cheng/McKay/Wang on resultants of composed polynomials. It considers composed polynomials of the form $f_i \circ (g_1, \ldots, g_{n+1})$, for $i = 1, \ldots, n$. That is, instead of f_i composed with only n polynomials, it considers f_i composed with $n+1$ polynomials. We call such polynomials "skewly composed" because the numbers of f_i's and g_j's do not agree. It is easy to see that the resultant of such skewly composed polynomials does not have such a nice factorization as in Jouanolou's and Cheng/McKay/Wang's case. Still, the resultant has some structure. The current paper finds that the resultant of such skewly composed polynomials is a certain nested resultant, where the inner resultant only depends on the polynomials $g_1, \ldots, g_{n+1}$ (see the main theorem, Theorem 1).

Next we outline the structure of the paper. Section 2 gives the main result of the paper and Section 3 proves it.

2. MAIN RESULT

We assume that the reader is familiar with the notion of projective (dense, Macaulay) resultant [23, 10]. As usual, we let the symbol $\mathrm{Res}_{k_1,\ldots,k_n}(h_1, \ldots, h_n)$ stand for the projective resultant of homogeneous polynomials $h_1, \ldots, h_n$ in the variables $(x_1, \ldots, x_n)$ of total degrees $k_1, \ldots, k_n$.

*Supported by the NSF grant CCF 0430741

ISSAC'06, July 9–12, 2006, Genova, Italy.

Furthermore, the symbols f_i denote homogeneous polynomials in the variables $y_1,\dots,y_{n+1}$ of total degrees $d_1,\dots,d_n$ and the symbols g_j denote homogeneous polynomials in the variables $(x_1,\dots,x_n)$ of total degrees e. Moreover, $f_i \circ (g_1,\dots,g_{n+1})$ denotes the composed polynomial obtained from f_i by replacing y_j with g_j for all j.

The main theorem contains three different resultants which eliminate different variables. The variables can be deduced from the context. Nevertheless, in order to avoid any confusion, we state the variables explicitly. That is, subsequently it is understood that the resultants

$$\mathrm{Res}_{d_1 e,\dots,d_n e}(h_1,\dots,h_n)$$

and

$$\mathrm{Res}_{e,\dots,e}(y_1g_2 - y_2g_1,\, y_1g_3 - y_3g_1,\dots,y_1g_{n+1} - y_{n+1}g_1)$$

eliminate the variables $(x_1,\dots,x_n)$. Whereas, the resultant

$$\mathrm{Res}_{d_1,\dots,d_n,\,e^{n-1}}(f_1,\dots,f_n,\,v)$$

eliminates the variables $(y_1,\dots,y_{n+1})$.

Now we are ready to state the main theorem.

THEOREM 1 (MAIN THEOREM). *Let h_i denote the composed polynomial $f_i \circ (g_1,\dots,g_{n+1})$, for $i = 1,\dots,n$. Then*

$$\mathrm{Res}_{d_1 e,\dots,d_n e}(h_1,\dots,h_n) = \mathrm{Res}_{d_1,\dots,d_n,\,e^{n-1}}(f_1,\dots,f_n,\,v),$$

where $v = (-1)^{n\,e^{n-1}} \times$

$$\frac{\mathrm{Res}_{e,\dots,e}(y_1g_2 - y_2g_1,\, y_1g_3 - y_3g_1,\dots,y_1g_{n+1} - y_{n+1}g_1)}{y_1^{(n-1)e^{n-1}}}.$$

REMARK 2. Naturally, one wants to know what object the expression v of Theorem 1 represents. The reader familiar with implicitization of surfaces may recognize this expression because it can be used for implicitization of certain surfaces [1]. Lemma 12 in Section 3 also studies the expression v. It shows that v is the toric resultant [10] of the polynomials $y_1 - g_1,\dots,y_{n+1} - g_{n+1}$. Computationally it is advantageous that this toric resultant can also be computed by a projective resultant via the formula for v. Since the projective resultant contains one polynomial less, it is expected that this formula can be used to more efficiently compute the toric resultant. (Also note that the denominator variable y_1 in v is arbitrarily chosen. From the proof in the next section it is obvious that one could derive similar formulas to have any other variable y_j in the denominator.)

EXAMPLE 3. Let $n = 3$ and f_1, f_2 and f_3 be homogeneous polynomials in the variables y_1, y_2, y_3, y_4 of respective total degrees $d_1 = 2$, $d_2 = 3$ and $d_3 = 4$. Furthermore, let g_1, g_2, g_3 and g_4 be 3-variate homogeneous polynomials of total degree $e = 5$. Furthermore, let h_i stand for the 3-variate homogeneous composed polynomial $f_i \circ (g_1, g_2, g_3, g_4)$. Then, by Theorem 1,

$$\mathrm{Res}_{10,15,20}(h_1,h_2,h_3) = \mathrm{Res}_{2,3,4,\,25}(f_1,f_2,f_3,\,v)$$

with

$$v = -\frac{\mathrm{Res}_{5,5,5}(y_1g_2 - y_2g_1,\, y_1g_3 - y_3g_1,\, y_1g_4 - y_4g_1)}{y_1^{50}}.$$

3. PROOF OF THE MAIN RESULT

Even though the statement of the main theorem, Theorem 1, does not require toric resultants [10], its proof benefits from toric resultant theory in Lemmas 6 and 9. Therefore we assume that the reader is familiar with the notion of toric resultant. The other lemmas in this section, besides Lemma 6 and 9, are designed to only use projective resultant theory which makes the proofs quite short.

Before we start proving, we state some necessary notation.

NOTATION 4. Let f_i stand for a homogeneous polynomial of total degree d_i in the variables $y_1,\dots,y_{n+1}$ with *independent symbolic coefficients*, for $i = 1,\dots,n$. Moreover, let g_j stand for a homogeneous polynomial of total degree e in the variables $x_1,\dots,x_n$ with *independent symbolic coefficients*, for $j = 1,\dots,n+1$. Moreover, let h_i be the composed polynomial $f_i \circ (g_1,\dots,g_{n+1})$.

NOTATION 5. In the subsequent lemmas we will study three different resultants for which we fix the following symbols.

- Let
$$r := \mathrm{Res}_{e,\dots,e}(y_1 - g_1,\dots,y_{n+1} - g_{n+1}),$$
where the y_j's are new independent symbols. Note that this resultant eliminates the variables x_i of the polynomials $y_j - g_j$.
- Let s stand for the toric resultant of the polynomials $y_j - g_j$ with respect to their natural supports $\mathcal{B}$ for the variables $x_1,\dots,x_n$. More precisely, $\mathcal{B}$ is the set of all exponent vectors for monomials in $x_1,\dots,x_n$ of total degree e and the origin $(0,\dots,0)$. Furthermore, we normalize the toric resultant of the polynomials $x_1^e,\dots,x_n^e, 1$ with respect to the supports $\mathcal{B}$ to be 1.
- Let
$$t := \mathrm{Res}_{e,\dots,e}(y_1g_2 - y_2g_1,\; y_1g_3 - y_3g_1,\dots,y_1g_{n+1} - y_{n+1}g_1).$$
Note that this resultant eliminates the variables x_i from the polynomials $y_1g_j - y_jg_1$.

We will see subsequently that it is important for the proof of the main theorem that the polynomials in Notations 4 and 5 have *independent symbolic coefficients*. This assumption allows to formulate statements such as *s is irreducible* in Lemma 6, where s is considered as a polynomial in the symbolic coefficients of the g_j's and in the symbols y_j.

Now we are ready to prove lemmas.

LEMMA 6. *We have $r = s^e$, where s is an irreducible polynomial, known as the toric resultant of the polynomials $y_1 - g_1,\dots,y_{n+1} - g_{n+1}$.*

PROOF. The formula $r = s^l$, follows directly from $(n+1)$ applications of Theorem 1 of [30], similarly to the proof of Corollary 5 of [30]. In this formula the exponent l is the lattice index of the integer lattice L generated by $\mathcal{B}$ in the lattice $\mathbb{Z}^{n+1}$ of all integer points. Since the volume of the fundamental parallelotope of the lattice $\mathbb{Z}^{n+1}$ is 1, the index l equals the volume of the fundamental parallelotope of the lattice L. Observe that the lattice L is generated by the vectors $(e,0,0,\dots,0)$, $(e-1,1,0,\dots,0)$, $(e-$

$1,0,1,\ldots,0),\ldots,(e-1,0,0,\ldots,1)$. Therefore the index l equals the determinant

$$\begin{vmatrix} e & e-1 & e-1 & \cdots & e-1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{vmatrix} = e.$$

□

The next lemma shows an important property of the support of the polynomial s.

LEMMA 7. *The polynomial s is homogeneous in $y_1,\ldots,y_{n+1}$ of degree e^{n-1}.*

PROOF. We determine the degree of the leading monomial of

$$p \;:=\; \mathrm{Res}_{\,e,\ldots,e}\,(\lambda\cdot y_1 \,-\, g_1,\ldots,\lambda\cdot y_{n+1} \,-\, g_{n+1})$$

in the new independent variable λ and show that this leading monomial divides p.

By the homogeneity, of degree $\gamma \;:=\; (n+1)\,e^n$, of the resultant p, and by the homogeneity of g_j, we have that p equals

$$\lambda^\gamma\ \mathrm{Res}_{\,e,\ldots,e}\left(y_1 - g_1(\lambda^{-\frac{1}{e}}\,x),\ldots,y_{n+1} - g_{n+1}(\lambda^{-\frac{1}{e}}\,x)\right),$$

where $g_j(\lambda^{-\frac{1}{e}}\,x)$ stands for g_j after substituting $\lambda^{-\frac{1}{e}}\,x_i$ for each variable x_i. Moreover, by the Poisson formula, we have that p equals

$$\lambda^\gamma\ \left(\mathrm{Res}_{\,e,\ldots,e}(g_2(\lambda^{-\frac{1}{e}}),\ldots,g_{n+1}(\lambda^{-\frac{1}{e}}))\right)^e\ \prod_\eta g_1(\lambda^{-\frac{1}{e}}\eta)\ =$$

$$\lambda^\gamma\ \left(\mathrm{Res}_{\,e,\ldots,e}(\lambda^{-1}g_2,\ldots,\lambda^{-1}g_{n+1})\right)^e\ \prod_\xi g_1(\xi)\ =$$

$$\lambda^{\gamma\,-\,n\,e^n}\ \ (\mathrm{Res}_{\,e,\ldots,e}(g_2,\ldots,g_{n+1}))^e\ \prod_\xi g_1(\xi)\ =$$

$$\lambda^{e^n}\ \mathrm{Res}_{\,e,\ldots,e}\,(y_1 - g_1,\ldots,y_{n+1} - g_{n+1})\,,$$

where η and ξ ranges over the common roots of

$$y_2 - g_2(\lambda^{-\frac{1}{e}}\,x),\ldots,y_{n+1} - g_{n+1}(\lambda^{-\frac{1}{e}}\,x)$$

and respectively of

$$y_2 - g_2,\ldots,y_{n+1} - g_{n+1}.$$

Thus p is a multiple of precisely one monomial in λ of degree e^n. Therefore by Lemma 6, the total degree of s in the y_j's is $\frac{e^n}{e}$. □

The statement of the next lemma requires the notion of specialized composed polynomials. By specialized composed polynomials $h_1,\ldots,h_n$ we mean that the symbolic coefficients of the f_i's and g_j's in the composed polynomials are replaced with actual constant values.

LEMMA 8. *For all specialized composed polynomials h_1, $\ldots,h_n$,*

$$\mathrm{Res}_{\,d_1,\ldots,d_n}\,(h_1,\ldots,h_n) \;=\; 0 \qquad (1)$$

implies that

$$\mathrm{Res}_{\,e,\ldots,e,\,e^{n-1}}\,(f_1,\ldots,f_n,\,s) \;=\; 0. \qquad (2)$$

PROOF. Assume that $\mathrm{Res}_{\,d_1,\ldots,d_n}\,(h_1,\ldots,h_n) \;=\; 0$. Then

$$\text{there is } (x_1,\ldots,x_n) \neq 0 \text{ with } g_1 = 0,\ldots,g_{n+1} = 0 \qquad (3)$$

or

$$\text{there is } (x_1,\ldots,x_n) \neq 0 \text{ and } (y_1,\ldots,y_{n+1}) \neq 0 \text{ with}$$
$$f_1 = \cdots = f_n \;=\; 0 \text{ and } g_1 = y_1,\ldots,g_{n+1} = y_{n+1}. \qquad (4)$$

Now, let V, W_1 and W_2 denote the algebraic set of polynomials $f_1,\ldots,f_n,\,g_1,\ldots,g_{n+1}$ satisfying (1), (3) and respectively (4). With this notation, we have that $V \subseteq W_1 \cup W_2$. Note that all the irreducible components of V are of co-dimension 1 and that W_1 is of co-dimension greater than 1. Thus $V \subseteq W_2$. Furthermore, note that by reordering existential quantifiers (4) implies that

$$\text{there is } (y_1,\ldots,y_{n+1}) \neq 0 \text{ with } (f_1 = \cdots = f_n \;=\; 0 \text{ and}$$
$$\text{there is } (x_1,\ldots,x_n) \neq 0 \text{ with } g_1 = y_1,\ldots,g_{n+1} = y_{n+1})$$

and that the latter implies (2) by Lemmas 7 and 6. □

The next lemma, Lemma 9, studies the resultant

$$\mathrm{Res}_{\,d_1,\ldots,d_n,\,e^{n-1}}\,(f_1,\ldots,f_n,\,s)$$

which is equal to $\mathrm{Res}_{\,d_1 e,\ldots,d_n e}\,(h_1,\ldots,h_n)$ of Theorem 1 as shown by Lemma 10.

LEMMA 9. *The polynomial $\mathrm{Res}_{\,d_1,\ldots,d_n,\,e^{n-1}}\,(f_1,\ldots,f_n,\,s)$ is the constant multiple of a power of an irreducible polynomial.*

PROOF. We identify the set of tuples of homogeneous polynomials $f_1,\ldots,f_n$ and $g_1,\ldots,g_{n+1}$ of the total degrees $d_1,\ldots,d_n$ and $e,\ldots,e$ with the corresponding space of coefficients. Furthermore, let V denote the set of tuples

$$(f_1,\ldots,f_n,\,g_1,\ldots,g_{n+1})$$

such that $\mathrm{Res}_{\,d_1,\ldots,d_n,\,e^{n-1}}\,(f_1,\ldots,f_n,\,s) \,=\, 0$. In order to show the lemma, we show that the algebraic set V is irreducible. To establish the latter, we show that a dense subset of V has a rational parametrization.

We construct a parametrizable set W whose algebraic closure is V as we will see below. Let $\tilde{f} \;=\; (f_1,\ldots,f_n)$, $\tilde{g} \;=\; (g_1,\ldots,g_{n+1})$, $\tilde{y} \;=\; (y_1,\ldots,y_{n+1})$, $\tilde{x} \;=\; (x_1,\ldots,x_n)$,

$$G_{\tilde{y}} \;=\; \{\tilde{g}\,|\,\text{there is } \tilde{x} \text{ with } x_n \neq 0$$
$$\text{such that } y_j - g_j = 0 \text{ for all } j\}$$

and $F_{\tilde{y}} \;=\; \left\{\tilde{f}\mid f_i = 0 \text{ for all } i\right\}$. Then we define W to be the union, over $\tilde{y}$ with $y_{n+1} \neq 0$, of $F_{\tilde{y}} \times G_{\tilde{y}}$. Next we show that V is the algebraic closure of W.

First we show that the algebraic closure of W is contained in V. This follows because W is a subset of V by Rojas' Vanishing Theorem [35, 16].

Next we show that V is contained in the algebraic closure of W. Let $S_{\tilde{y}}$ be the set of $\tilde{g}$'s such that $s = 0$. Furthermore, let the set Z be the union, over $\tilde{y}$ with $y_{h+1} \neq 0$, of $F_{\tilde{y}} \times S_{\tilde{y}}$. We first show that the algebraic closure of Z is contained in the algebraic closure of W and then that the algebraic closure of Z equals V.

We start with observing that, for fixed $\tilde{y}$, the algebraic closure of $G_{\tilde{y}}$ is the set $S_{\tilde{y}}$. (In more detail, notice that the algebraic closure of the set $C \;=\; \bigcup_{\tilde{y}}\ \{\tilde{y}\}\times G_{\tilde{y}}$ is $\bigcup_{\tilde{y}}\ \{\tilde{y}\}\times S_{\tilde{y}}$

by the definition of the toric resultant and by Rojas' Vanishing Theorem. Moreover notice that the algebraic closure of C is also $\bigcup_{\tilde{y}} \{\tilde{y}\} \times \overline{G_{\tilde{y}}}$, where $\overline{G_{\tilde{y}}}$ is the algebraic closure of $G_{\tilde{y}}$. Since the sets $\{y\} \times \overline{G_{\tilde{y}}}$ are pairwise disjoint, $\overline{G_{\tilde{y}}}$ equals $S_{\tilde{y}}$.) Thus any polynomial that vanishes on W also vanishes on Z. Therefore the algebraic closure of Z is contained in the algebraic closure of W.

Now, let I be the union, over $\tilde{y} \neq 0$ with $y_{n+1} = 0$, of $F_{\tilde{y}} \times S_{\tilde{y}}$. By Rojas' Vanishing Theorem we have that $V = Z \cup I$ where $Z \not\subseteq I$ and $I \not\subseteq Z$. Also observe that I is of co-dimension greater than 1. Furthermore, let R be $\mathrm{Res}_{d_1,\ldots,d_n,\, e^{n-1}}(f_1,\ldots,f_n,\, s)$ and suppose that R can be factored into a product $p \cdot q$ of polynomials such that p vanishes on Z but not on V and q vanishes on I but not on V. Without loss of generality we assume p and q do not have a polynomial factor in common. Now, the factorization $p \cdot q$ implies that the set V has at least two distinct components of co-dimension 1, the first one being the algebraic closure of Z and the second one being the algebraic closure of I. However, this is impossible because I is of co-dimension greater than 1. Therefore any factor of R that vanishes on Z also vanishes on I. Therefore the algebraic closure of Z is V.

In order to obtain a rational parametrization of W we solve for certain coefficients of f_i and g_j in the equations $f_i = 0$ and $y_j - g_j = 0$. (See also [21] for another use of this idea.) Now, let a_i, b_j be the coefficient of $y_{n+1}^{d_i}$ in f_i and, respectively, of x_n^e in g_j. Furthermore, let $\overline{f}_i$ be $a_i\, y_{n+1}^{d_i} - f_i$ and $\overline{g}_j$ be $b_j\, x_n^e - g_j$. Then a rational parametrization of W (and hence V) is given by $a_i = \frac{\overline{f}_i}{y_{n+1}^{d_i}}$ and $b_j = \frac{\overline{g}_j}{x_n^e}$ where the variables x_i, y_j and the coefficients besides the a_i's and b_j's are considered as unconstrained parameters. □

The next lemma is a first version of the main theorem, Theorem 1. Subsequently, we will still convert the resultant s into a resultant of fewer polynomials in fewer variables.

LEMMA 10. *We have*

$$\mathrm{Res}_{d_1 e,\ldots,d_n e}(h_1,\ldots,h_n) = \mathrm{Res}_{d_1,\ldots,d_n,\, e^{n-1}}(f_1,\ldots,f_n,\, s). \quad (5)$$

PROOF. Let q_1 stand for the left-hand side of (5) and let q_2 stand for the right-hand side of (5).

By Lemma 8 and by Hilbert's Nullstellensatz, $q_2^\delta = p\, q_1$, for some positive integer δ and some polynomial p. Since q_2 is the constant multiple of the power of an irreducible polynomial (Lemma 9),

$$q_1 = \lambda\, q_2^\epsilon, \quad (6)$$

for some constant λ and some rational number ϵ.

Next we determine λ in (6) by specializing the f_i's and g_j's in (6). Replace f_i with $y_i^{d_i}$ and g_j with x_j^e, for $j = 1,\ldots,n$. Then $q_1 = 1$. Furthermore, replace g_{n+1} with 0. Then by Lemma 6, $s = y_{n+1}^{e^{n-1}}$ and therefore $q_2 = 1$. Thus $\lambda = 1$.

Next we determine ϵ in (6) by comparing the total degrees in f_1 of q_1 and q_2. These total degrees are $d_2 e \cdots d_n e$ and respectively $d_2 \cdots d_n\, e^{n-1}$ which are equal. Hence, $\epsilon = 1$. □

The next lemmas convert the resultant s into a resultant of fewer polynomials in fewer variables.

Similarly to Lemma 8, the y_j's and the symbolic coefficients of the g_j's are specialized with constant values in the statement of Lemma 11.

LEMMA 11. *For all constants $y_1,\ldots,y_{n+1}$ and for all polynomials $g_1,\ldots,g_{n+1}$, we have that $t = 0$ implies that $y_1 = 0$ or $s = 0$.*

PROOF. Assume $t = 0$ for fixed y_j's and g_j's. If $y_1 = 0$, then

$$t = \mathrm{Res}_{e,\ldots,e}(-y_2 g_1,\, -y_3 g_1,\ldots,-y_{n+1} g_1) = 0.$$

Next assume $y_1 \neq 0$. Then there is a tuple $(x_1,\ldots,x_n) \neq 0$ with $y_1\, g_j - y_j g_1 = 0$, for all j. Now, let $k := \frac{g_1}{y_1}$ for such $(x_1,\ldots,x_n)$. Then $g_j = k\, y_j$. If $k = 0$, that is, $g_1 = 0$, then $g_j = 0$, for all j, and $r = s = 0$ by Lemma 6. If $k \neq 0$, then by the homogeneity of the g_j's and by Lemma 6, $r = s = 0$. □

The next lemma is not only a cornerstone for the main theorem. It is also of independent interest. That is, it shows that the toric resultant of the $n+1$ polynomials $y_j - g_j$, for $j = 1,\ldots,n+1$ can be computed as the projective resultant of n polynomials.

LEMMA 12. *We have $t = (-1)^{n\, e^{n-1}}\, s\, y_1^{(n-1)e^{n-1}}$.*

PROOF. By Lemma 11, $t = 0$ implies that $s\, y_1 = 0$. By Hilbert's Nullstellensatz, $(s y_1)^\gamma = p\, t$, for some positive integer γ and some polynomial p. Since s is irreducible by Lemma 6,

$$t = \lambda\, s^\delta\, y_1^\epsilon, \quad (7)$$

for a constant λ and integers δ and ϵ.

We determine the values of λ, δ and ϵ in (7) by specializing g_1 to 0. Then

$$t = \mathrm{Res}_{e,\ldots,e}(y_1 g_2,\, y_1 g_3,\ldots,y_1 g_{n+1}) = y_1^{n\, e^{n-1}}\, \mathrm{Res}_{e,\ldots,e}(g_2,\, g_3,\ldots,g_{n+1}).$$

Furthermore, by Lemma 9 of [28],

$$\begin{aligned} r &= \mathrm{Res}_{e,\ldots,e}(y_1,\, y_2 - g_2,\ldots,y_{n+1} - g_{n+1}) = \\ &\mathrm{Res}_{e,\ldots,e}(1,\, y_2 - g_2,\ldots,y_{n+1} - g_{n+1})\; y_1^{e^n} = \\ &(\mathrm{Res}_{e,\ldots,e}(-g_2,\ldots,-g_{n+1}))^e\; y_1^{e^n} = \\ &(-1)^{n\, e^n}\; (\mathrm{Res}_{e,\ldots,e}(g_2,\ldots,g_{n+1}))^e\; y_1^{e^n} \end{aligned}$$

and thus by Lemma 6,

$$s = (-1)^{n e^{n-1}}\, \mathrm{Res}_{e,\ldots,e}(g_2,\ldots,g_{n+1})\, y_1^{e^{n-1}}.$$

Therefore $\lambda = (-1)^{n\, e^{n-1}}$, $\delta = 1$ and $\epsilon = (n-1)e^{n-1}$. □

REMARK 13. Note that (7) also follows from [1]. Thus one could avoid using Lemma 11. However, since the proof of this lemma is short we include it in the present paper in order to make the paper as self-contained as possible.

Now we are ready to prove the main theorem.

PROOF OF THEOREM 1. Note that Lemmas 5 and 12 are stable under specialization of the symbolic coefficients of the f_i's and g_j's. Thus, by combining the two lemmas, we have shown the main result, Theorem 1. □

4. CONCLUSION AND OUTLOOK

We gave a formula for the resultant of skewly composed polynomials, obtained by composing n homogeneous polynomials with $n+1$ homogeneous polynomials. Future work might study resultants of other skewly composed polynomials, obtained by composing n homogeneous polynomials with $k > n+1$ homogeneous polynomials. It is still an open question if Theorem 1 can be generalized to such cases.

Acknowledgments

The author thanks Josef Schicho and the anonymous reviewers for information leading to improvements of the paper.

5. REFERENCES

[1] L. Busé and C. D'Andrea. Inversion of parameterized hypersurfaces by means of subresultants. In *ISSAC 2004*, pages 65–71. ACM, New York, 2004.

[2] L. Busé, M. Elkadi, and B. Mourrain. Generalized resultants over unirational algebraic varieties. *J. Symbolic Computation*, 29(4-5):515–526, 2000.

[3] J. Canny and I. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3):417–451, May 2000.

[4] J. Canny, E. Kaltofen, and L. Y. Solving systems of non-linear polynomial equations faster. In *Proc. ACM-SIGSAM 1989 Internat. Symp. Symbolic Algebraic Comput. ISSAC'89*, pages 121–128. ACM, 1989.

[5] E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *J. Math. Sci. Univ. Tokyo*, 5(1):119–148, 1998.

[6] A. Cayley. On the theory of elimination. *Cambridge and Dublin Math. J.*, 3:116–120, 1848.

[7] M. Chardin. *Contributions à l'algèbre commutative effective et à la théorie de l'élimination*. PhD thesis, Université Paris VI, 1990.

[8] C. C. Cheng, J. H. McKay, and S. S. Wang. A chain rule for multivariable resultants. *Proceedings of the American Mathematical Society*, 123(4):1037–1047, April 1995.

[9] A. Chtcherba, D. Kapur, and M. Minimair. Cayley-Dixon resultant matrices of multi-univariate composed polynomials. In V. Ganzha and E. Mayr, editors, *Computer Algebra in Scientific Computing*, volume 3718 of *Lecture Notes in Computer Science*, pages 125–137, Berlin Heidelberg, 2005. Springer Verlag. 8th International Workshop, CASC 2005, Kalamata, Greece, September 2005, Proceedings.

[10] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer Verlag, New York, Berlin, Heidelberg, 2nd edition, 2004.

[11] C. D'Andrea and A. Dickenstein. Explicit formulas for the multivariate resultant. *Pure Appl. Algebra*, 164(1-2):59–86, 2001.

[12] A.-L. Dixon. The eliminant of three quantics in two independent variables. *Proc. London Math. Soc.*, 7:49–69, 473–492, November 1908.

[13] I. Z. Emiris and V. Pan. The structure of sparse resultant matrices. In *Proc. Int. Symp. on Symbolic and Algebraic Computation (ISSAC)*. ACM Press, 1997.

[14] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser, Boston, 1994.

[15] L. González-Vega. Une théorie des sous-résultants pour les polynômes en plusieurs variables. *C. R. Acad. Sci. Paris Sér. I Math.*, 313/13:905–908, 1991.

[16] H. Hong and M. Minimair. Sparse resultant of composed polynomials I. *J. Symbolic Computation*, 33:447–465, 2002.

[17] J. P. Jouanolou. Le formalisme du résultant. *Adv. Math.*, 90(2):117–263, 1991.

[18] D. Kapur and T. Saxena. Sparsity considerations in Dixon resultants. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (Philadelphia, PA, 1996)*, pages 184–191, New York, 1996. ACM.

[19] D. Kapur and T. Saxena. Extraneous factors in the Dixon resultant formulation. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 141–148, New York, 1997. ACM.

[20] A. Khetan. The resultant of an unmixed bivariate system. *J. Symbolic Comput.*, 36(3-4):425–442, 2003.

[21] J. König. *Einleitung in die allgemeine Theorie der algebraischen Gröszen*. B. G. Teubner, Leipzig, Germany, 1903.

[22] R. Lewis and P. Stiller. Solving the recognition problem for six lines using the Dixon resultant. *Math. Comput. Simulation*, 49(3):205–219, 1999.

[23] F. S. Macaulay. *The algebraic theory of modular systems*. Cambridge Mathematical Library, 1916.

[24] D. Manocha and J. Canny. Multipolynomial resultant algorithms. *J. Symbolic Computation*, 15(2):99–122, 1993.

[25] J. H. McKay and S. S. Wang. A chain rule for the resultant of two polynomials. *Arch. Math.*, 53(4):347–351, 1989.

[26] J. H. McKay and S. S. Wang. A chain rule for the resultant of two homogeneous polynomials. *Arch. Math.*, 56(4):352–361, 1991.

[27] M. Minimair. Sparse resultant of composed polynomials II. *J. Symbolic Computation*, 33:467–478, 2002.

[28] M. Minimair. Dense resultant of composed polynomials. *J. Symbolic Computation*, 36(6):825–834, December 2003.

[29] M. Minimair. Factoring resultants of linearly combined polynomials. In J. R. Sendra, editor, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 207–214, New York, NY, 2003. ACM. ISSAC 2003, Philadelphia, PA, USA, August 3-6, 2003.

[30] M. Minimair. Sparse resultant under vanishing coefficients. *J. Algebraic Combinatorics*, 18(1):53–73, July 2003.

[31] M. Minimair. Computing resultants of partially composed polynomials. In V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing. Proceedings of the CASC 2004 (St. Petersburg, Russia)*, pages 359–366. TUM München, 2004.

[32] M. Minimair. Resultants of partially composed polynomials. *J. Symbolic Computation*, 2005.

[33] G. Nakos and R. M. Williams. Elimination with the Dixon resultant. *Mathematica for Education and Research*, 6/3:11–21, 1997.

[34] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Mathematische Zeitschrift*, 214:377–396, 1993.

[35] J. M. Rojas. Solving degenerate sparse polynomial systems faster. *J. Symbolic Computation*, 28(1 and 2):155–186, July/August 1999. Special Issue Polynomial Elimination – Algorithms and Applications.